IN THE DRAWINGS:

Please replace the attached Replacement Sheet for its corresponding drawing sheet in the present Application. The Replacement Sheet includes the "211" indicator.

REMARKS

Applicant appreciates the time taken by the Examiner to review Applicant's present application. This application has been carefully reviewed in light of the Official Action mailed February 3, 2005. Applicant respectfully requests reconsideration and favorable action in this case.

Drawing Objections

The drawings stand objected to as failing to comply with 37 C.F.R. § 1.84(p)(5). The drawing of Fig. 2, includes reference number 211. Accordingly, withdrawal of this objection is respectfully requested.

Rejections under 35 U.S.C. § 103

Claims 1-26 stand rejected as obvious over U.S. Patent No. 6,247,127 ("Vandergeest") in view of U.S. Patent No. 4,630,201 ("White").

In order to establish a *prima facie* case of obviousness, the Examiner must show: that (1) the prior art references teach or suggest all of the claim limitations, (2) that there is some suggestion or motivation in the references (or within the knowledge of one of ordinary skill in the art) to modify or combine the references and (3) that there is a reasonable expectation of success. M.P.E.P. 2142, 2143; In re Vaeck, 947 F.2d 488, 20 U.S.P.Q.2d 1438 (Fed. Cir. 1991). The Examiner must explain with reasonable specificity at least one rejection – otherwise, the Examiner has failed procedurally to establish a *prima facie* case of obviousness. M.P.E.P. 2142; Ex parte Blanc, 13 U.S.P.Q.2d 1383 (Bd. Pat Application. & Inter. 1989). When the motivation to combine the teachings of the references is not immediately apparent, it is the duty of the Examiner to explain why the combination of the teachings is proper. Ex parte Skinner, 2 U.S.P.Q.2d 1788, 1790 (Bd. Pat. App. & Inter. 1986).

Applicants respectfully submit that the Examiner has failed to establish a *prima facie* case of obviousness as the references do not disclose, teach, or suggest all of the claim limitations of Claims 1-26. More particularly, the references do not disclose, teach or suggest a method of conducting a secure transaction with an on-line service while offline including i)

"issuing a transaction authorization token to a user from an application server for the on-line service while the user is online," ii) "preparing an off-line transaction object containing data to specify and request the transaction" and iii) "sending a message to the on-line service, said message containing the transaction object and the authorization token."

Claim 1 recites:

> [a] method of conducting a secure transaction with an on-line service while offline comprising the steps of issuing a transaction authorization token to a user from an application server for the on-line service while the user is online; preparing an off-line transaction object containing data to specify and request the transaction; sending a message to the on-line service, said message containing the transaction object and the authorization token; upon receipt of the message, the application server validating the token to authenticate the user and to authorize the transaction; and executing the transaction object if the transaction is authorized.

Claim 1 recites a method of conducting a secure transaction with an on-line service which enables off-line transactions with substantially the same security as PKI, without the requirement of secure network connectivity, and without the need for special PKI software to be run by the end user (Specification – page 3 – lines 13-15). The method includes i) "issuing a transaction authorization token to a user from an application server for the on-line service while the user is online," ii) "preparing an off-line transaction object containing data to specify and request the transaction" and iii) "sending a message to the on-line service, said message containing the transaction object and the authorization token. These features of the present invention allow a user to conduct part of a secure transaction (i.e., prepare the transaction object) with an on-line service while off-line (i.e., not connected to the on-line service).

Vandergeest does not teach a method of conducting secure transactions with an on-line service while off-line from the on-line service. Although Vandergeest discusses offline transactions, the term offline appears to refer to the security server rather than to the on-line service with which the secure transaction is to be performed. Thus, Vandergeest teaches a method for conducting secure transactions with a targeted communications entity while off-line from a security information repository, not an on-line service with which the transaction is being performed (Vandergeest – abstract).

Furthermore, Vandergeest teaches an end-user going online with a security information repository and requesting from the security information repository security information relating to at least one targeted communication entity. Upon receiving the security information, the end-user updates a local security information repository and goes off-line from the security information repository. While off-line with the security information repository, the user

processes communications with the at least one targeted communications entity based upon the security information that is stored in the user's local security information repository. (Vandergeest – col. 2, lines 50-65). Thus, Vandergeest teaches a method to allow users to go off-line from a security information repository, yet continue secure communications with a targeted communications entity. (Vandergeest – col. 3, lines 3-4). Vandergeest does not teach or suggest issuing a transaction authorization token to a user from an application server for the on-line service as the security information is received from the third-party security information repository, not the applications server for the on-line service.

The Examiner points to col. 4, lines 8-16 of Vandergeest for evidence of the claimed limitation of issuing a transaction authorization token to a user from an application server for the on-line service while the user is online. However, this passage of Vandergeest appears to provide evidence that an end-user would request security information from a security repository not an online service with which the user wishes to engage in secured transactions. Such security information received from a security repository cannot be properly construed as the claimed transaction authorization token issued by an application server of an on-line service. Thus, the cited passage does not teach issuing a transaction authorization token to a user from an application server for the on-line service while the user is online as claimed.

Further, Vandergeest does not teach preparing an off-line transaction object containing data to specify and request the transaction. The Examiner points to col. 4, lines 18-20 and col. 5, lines 15-22 of Vandergeest for evidence of the claimed limitation of preparing an off-line transaction object containing data to specify and request the transaction. However, the first passage appears to teach the security information (e.g., public key certificates, cross certificates, and revocation lists) requested from a security repository and stored to an end-user's local security information repository just prior to the end-user going off line from the security information repository. The second passage appears to teach that a target communication entity will allow communications with the end-user if the end-user is in possession of correct security information. Again, to the extent "offline" is used, it refers to the security server not the on-line service with which the user wishes to securely communicate. Thus, the cited passage does not teach preparing an off-line transaction object containing data to specify and request the transaction.

Therefore, Vandergeest cannot be properly construed as teaching or suggesting the claimed method of conducting a secure transaction with an on-line service while offline. The

cited passages do not teach issuing a transaction authorization token to a user from an application server for the on-line service while the user is online. Nor do the cited passages teach preparing an off-line transaction object containing data to specify and request the transaction. Further, there is no motivation to modify Vandergeest such that the claimed limitations are met. Furthermore, there is no motivation to combine references such that the claimed limitations are met. Regardless, combination of the Vandergeest and White references do not teach the claimed limitations.

White does not remedy deficiencies of Vandergeest such that their combination teaches the claimed method of conducting secure transactions with an on-line service while off-line from the on-line service. In particular, White does not teach issuing a transaction authorization token to a user from an application server for the on-line service while the user is online. Further, Applicants respectfully traverse the Examiner's assertion that White teaches sending a message to the on-line service, said message containing the transaction object and the authorization token; upon receipt of the message, the application server validating the token to authenticate the user and to authorize the transaction; and executing the transaction object if the transaction is authorized. In contrast to the claimed limitations, White teaches a security system for use in an electronic funds transfer environment which is of particular use in promoting security in off-line check writing situations (White – abstract).

The Examiner points to figure 2B and col. 7, line 60 through col. 8 line 9 of White for evidence of the claimed limitation of sending a message to the on-line service, said message containing the transaction object and the authorization token; upon receipt of the message, the application server validating the token to authenticate the user and to authorize the transaction; and executing the transaction object if the transaction is authorized. However, this passage of White appears to describe a method of preventing unauthorized or fraudulent check-writing, where a check is a typical paper instrument used to draw monetary funds from a banking account. The method of White includes creating an authentication method for check cashing which is reliant upon a security code number for each check where the security code number is a function of the check amount and a random number assigned to the check number. The security code number is generated by a portable transactor, not an applications server of an on-line transaction. Thus, an end-user having a transactor using an algorithm would print a security code number on a check at time of issuance, and the security code number would be verified by the bank before the check would be paid. Therefore, the portable transactor, not an application server associated with an online service, issues the security code. Thus, Applicants

submit that printing a generated security code on a paper using a portable transactor is not issuing a transaction authorization token to a user from an application server for an on-line service. Consequently, White does not teach the claimed issuing a transaction authorization token to a user from an application server for the on-line service while the user is online. Therefore, White cannot remedy this deficiency in Vandergeest.

Further, Applicants respectfully traverse the Examiner's assertion that White teaches sending a message to the on-line service, said message containing the transaction object and the authorization token; upon receipt of the message, the application server validating the token to authenticate the user and to authorize the transaction; and executing the transaction object if the transaction is authorized. Because White deals with security numbers generated by transactors and printed on physical bank checks which will be presented to banks physically, White cannot be properly construed as teaching or suggesting sending a message to an on-line service. Further, there is no motivation to modify White such that the claimed limitations are met.

Applicants respectfully submit that the Examiner has failed to establish a *prima facie* case of obviousness for Claims 1-26 as the prior art references do not disclose, teach or suggest all of the claim limitations. Specifically, the prior art cited by the Examiner does not appear to teach i) "issuing a transaction authorization token to a user from an application server for the on-line service while the user is online," ii) "preparing an off-line transaction object containing data to specify and request the transaction" and iii) "sending a message to the on-line service, said message containing the transaction object and the authorization token." While the Examiner has provided passages of Vandergeest and White to attempt to show where these limitations are found, Applicants respectfully submit that the cited art does not disclose or teach the claimed limitations, as discussed above in relation to the § 103 rejections. Accordingly, Applicants respectfully request withdrawal of this rejection and allowance of Claims 1-26.

Applicants have now made an earnest attempt to place this case in condition for allowance. Other than as explicitly set forth above, this reply does not include an acquiescence to statements, assertions, assumptions, conclusions, or any combination thereof in the Office Action. For the foregoing reasons and for other reasons clearly apparent, Applicants respectfully request full allowance of Claims 1-26. The Examiner is invited to telephone the undersigned at the number listed below for prompt action in the event any issues remain.

The Director of the U.S. Patent and Trademark Office is hereby authorized to charge any fees or credit any overpayments to Deposit Account No. 50-3183 of Sprinkle IP Law Group.

Respectfully submitted,

Sprinkle IP Law Group
Attorneys for Applicant

John L. Adair
Reg. No. 48,828

Date: 5/3/05

1301 W. 25th Street, Suite 408
Austin, TX 78705
Tel. (512) 637-9220
Fax. (512) 371-9088